PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-223689
(43)Date of publication of application : 17.08.2001

(51)Int.Cl. H04L 9/20
H04Q 7/38

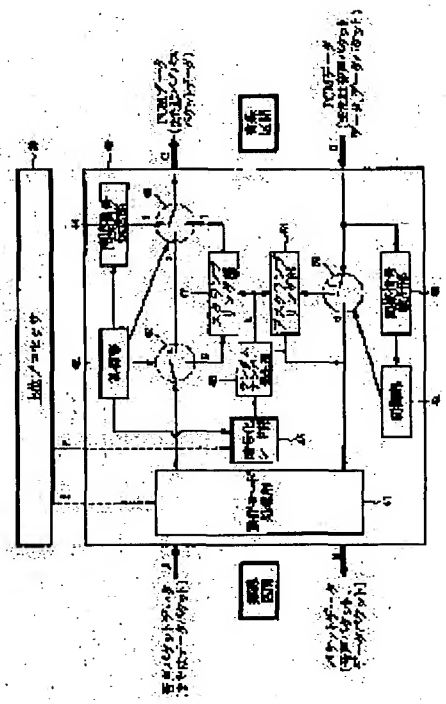
(21)Application number : 2000-376109
(22)Date of filing : 11.12.2000

(71)Applicant : HYNIX SEMICONDUCTOR INC
(72)Inventor : BOKU SEICHIN

(30)Priority
Priority number : 1999 9958711 Priority date : 17.12.1999 Priority country : KR

(54) VOICE AND DATA ENCRYPTION/DECODING UNIT FOR MOBILE COMMUNICATION SYSTEM AND ITS METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a voice and data encryption/decoding unit in a mobile communication system, that can prevent wire tapping and to provide its method.
SOLUTION: The unit for encrypting/decoding voice/data and its method in a mobile communication system subjects VOCODing or bypassing a signal sent from a wireless channel block to scramble the VOCODing and bypassed signal, through the use of a random number and transmit the scrambled signal to a wired channel block. Furthermore, the scrambled signal received from the wired channel block is descrambled according to the random number, depending on the presence of detection of a synchronizing signal, vocoded or bypassed and sent to the wireless channel block. Thus, maintainability in the wired channel block between the system and the vocoder can be maintained considerably, so as to prevent wire tapping in advance.



LEGAL STATUS

[Date of request for examination] 11.12.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－223689
（P2001－223689A）
(43)公開日　平成13年８月17日(2001.8.17)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/20		Ｈ０４Ｌ　9/00		６５３
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26		１０９Ｒ

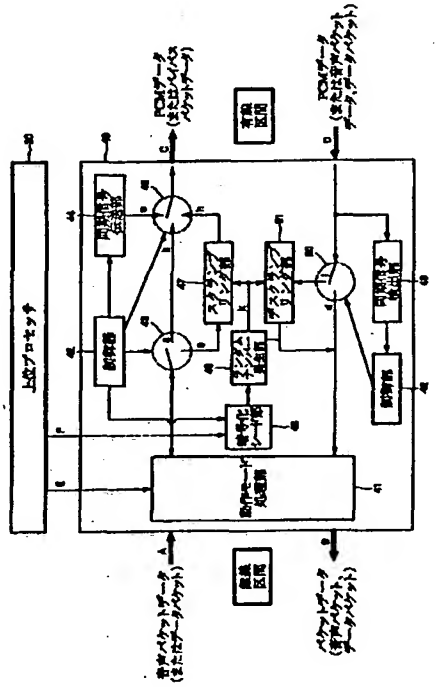
審査請求　有　　請求項の数12　ＯＬ　（全 10 頁）

(21)出願番号　特願2000－376109(P2000－376109)
(22)出願日　平成12年12月11日(2000.12.11)
(31)優先権主張番号　１９９９－５８７１１
(32)優先日　平成11年12月17日(1999.12.17)
(33)優先権主張国　韓国（ＫＲ）

(71)出願人　591024111
株式会社ハイニックスセミコンダクター
大韓民国京畿道利川市夫鉢邑牙美里山136－１
(72)発明者　朴　正　鎭
大韓民国京畿道利川市夫鉢邑牙美里山136－１
(74)代理人　100057874
弁理士　曾我　道照　（外６名）

(54)【発明の名称】　移動通信システムの音声及びデータ暗号化／復号化装置及びその方法

(57)【要約】
【課題】　盗聴を防止できるようにした移動通信システムにおける音声及びデータ暗号化／復号化装置及びその方法を提供する。
【解決手段】　本発明による移動通信システムの音声／データを暗号化／復号化するための装置及びその方法は、無線チャネル区間から伝送されてきた信号をボコーディングまたはバイパスさせた後、ボコーディングまたはバイパスされた信号をランダムナンバーを利用してスクランブリングして有線チャネル区間に伝送する。また、有線チャネル区間から受信されるスクランブリングされた信号を同期信号の検出有無によりランダムナンバーでデスクランブリングした後、ボコーディングまたはバイパスさせて無線チャネル区間に伝送する。こうようにすることで、システムボコーダ間有線チャネル区間における保安性を画期的に維持させ盗聴を未然に防止できる。



【特許請求の範囲】

【請求項１】　移動通信システムの音声／データボコーディング装置において、
音声及びデータの動作モードを制御する動作モード制御信号、データ暗号化のための暗号化キー供給制御信号、同期信号発生制御信号を生じる制御部と、
前記制御部から発生した動作モード制御信号により無線チャネル区間から伝送されてきた音声／データパケットをボコーディングしたりバイパスさせる動作モード処理部と、
前記制御部から発生した暗号化キー供給制御信号によりランダムナンバーを発生させるランダムナンバー発生部と、
前記制御部から発生した同期信号発生制御信号により同期信号を生じて有線チャネル区間に伝送する同期信号伝送部と、
前記ランダムナンバー発生部から発生したランダムナンバーを利用して前記動作モード処理部でボコーディングまたはバイパスされたＰＣＭまたは音声／データパケットを暗号化した後、前記同期信号の伝送が完了すると、有線チャネル区間に伝送する暗号化部とを含んで構成されたことを特徴とする移動通信システムの音声及びデータ暗号化装置。

【請求項２】　前記制御部の制御信号により同期信号発生部にスイッチングされて発生した同期信号を有線チャネル区間に伝送した後、同期信号の伝送が完了すると提供される制御信号により前記暗号化部にスイッチングされて暗号化された信号を有線チャネル区間に伝送するスイッチング部をさらに備えることを特徴とする請求項１記載の移動通信システムの音声及びデータ暗号化装置。

【請求項３】　前記制御部の制御信号により貯蔵された暗号化キーを前記ランダムナンバー発生部に供給する暗号化キー供給部をさらに備えることを特徴とする請求項１記載の移動通信システムの音声及びデータ暗号化装置。

【請求項４】　前記ランダムナンバー発生部から発生したランダムナンバーは、前記動作モード処理部でボコーディングされたＰＣＭまたはバイパスされた音声／データパケットデータを暗号化するための任意の位置情報であることを特徴とする請求項１記載の移動通信システムの音声／データ暗号化装置。

【請求項５】　移動通信システムの音声及びデータボコーディング装置において、
有線チャネル区間から伝送されてきた暗号化された信号から同期信号を検出する同期信号検出部と、
前記同期信号検出部で同期信号が検出されると、前記復号化制御信号及び動作モード制御信号を提供して、復号化キーを供給できるように制御信号を提供する制御部と、
前記制御部から提供される復号化キーによりランダムナンバーを生じるランダムナンバー発生部と、
前記制御部から提供される復号化制御信号により前記ランダムナンバー発生部から発生したランダムナンバーで有線チャネルから受信された暗号化された信号を復号化する復号化部と、
前記制御部から提供される動作モードにより前記復号化部で復号化されたＰＣＭをボコーディングしてパケットに変換したりまたは音声／データパケットをそのままバイパスさせた後、無線チャネル区間に伝送する動作モード処理部とを含んで構成されたことを特徴とする移動通信システムの音声／データ復号化装置。

【請求項６】　前記制御部から提供される制御信号により有線チャネルから伝送されてきた暗号化された信号を前記復号化部にスイッチングするスイッチング部をさらに備えることを特徴とする請求項５記載の移動通信システムの音声及びデータ復号化装置。

【請求項７】　前記制御部の制御信号により貯蔵された暗号化キーを前記ランダムナンバー発生部に供給する復号化キー供給部をさらに備えることを特徴とする請求項５記載の移動通信システムの音声及びデータ暗号化方法。

【請求項８】　前記ランダムナンバー発生部から発生したランダムナンバーは、前記有線チャネル区間から受信したＰＣＭまたは音声／データパケットデータを復号化するための任意の位置情報であることを特徴とする請求項５記載の移動通信システムの音声／データ暗号化装置。

【請求項９】　移動通信システムの音声／データボコーディング装置において、
無線チャネル区間から伝送されてきた音声／データパケットを提供される動作モード信号によりボコーディングしたりバイパスさせて、復号化されたＰＣＭまたはパケットを提供される動作モードによりボコーディングまたはバイパスさせて無線チャネル区間に伝送する動作モード処理部と、
供給される暗号化及び復号化キーによりランダムナンバーを発生させるランダムナンバー発生部と、
提供される制御信号により同期信号を生じて有線チャネル区間に伝送する同期信号伝送部と、
前記ランダムナンバー発生部から発生したランダムナンバーを利用して前記動作モード処理部でボコーディングまたはバイパスされたＰＣＭまたは音声／データパケットを暗号化した後、前記同期信号の伝送が完了すると、有線チャネル区間に伝送する暗号化部と、
有線チャネル区間から伝送されてきた暗号化された信号から同期信号を検出する同期信号検出部と、
提供される復号化制御信号により前記ランダムナンバー発生部から発生したランダムナンバーにより有線チャネルから受信された暗号化された信号を復号化する復号化部と、

前記同期信号検出部で同期信号が検出されると、前記復号化部に復号化制御信号を提供して、前記暗号化キー及び復号化キーを供給できるように制御信号を提供して、前記同期信号発生制御信号を提供する制御部とで構成されたことを特徴とする移動通信システムの音声及びデータ暗号化／復号化装置。

【請求項１０】　前記制御部の制御信号により貯蔵された暗号化キー及び復号化キーを前記ランダムナンバー発生部に供給する復号化キー供給部をさらに備えることを特徴とする請求項９記載の移動通信システムの音声及びデータ暗号化／復号化方法。

【請求項１１】　移動通信システムの音声及びデータボコーディング方法において、

無線チャネル区間から伝送されてきた音声パケットまたはデータパケットを提供される動作モードによりボコーディングまたはバイパスさせた後出力する段階と、

暗号化キー情報により任意の一定なランダムナンバーを生じる段階と、

同期信号を生成してその生成した同期信号を有線チャネル区間に伝送する段階と、

前記同期信号が伝送されると前記発生したランダムナンバーを利用して前記モード処理された信号（ＰＣＭまたはバイパスされた音声パケットまたはバイパスされたデータパケット）を暗号化した後、暗号化された信号を有線チャネル区間に伝送する段階とで構成されることを特徴とする移動通信システムの音声及びデータ暗号化方法。

【請求項１２】　移動通信システムの音声及びデータボコーディング方法において、

有線チャネル区間から暗号化された信号を受信する段階と、

暗号化された信号が受信されると、その暗号化された信号から同期信号を検出する段階と、

前記同期信号が検出されると、復号化キーにより任意の一定なランダムナンバーを生じる段階と、

前記発生したランダムナンバーにより前記暗号化された信号を復号化する段階と、

前記復号化されたＰＣＭまたはパケットを動作モードによりボコーディングまたはバイパスさせてパケットに変換した後、無線チャネル区間に伝送する段階とで構成されることを特徴とする移動通信システムにおける音声及びデータ復号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、移動通信システムの音声及びデータボコーディングに関するもので、特に、デジタル移動通信システムのボコーディング装置で移動加入者間音声通話及びデータ通信時システム内ボコーダの動作モードに関係なく有線チャネル上の通信信号を暗号化及び復号化するための移動通信システムにおける音声及びデータ暗号化／復号化装置及びその方法に関するものである。

【０００２】

【従来の技術】一般に、デジタル移動通信システムで制限された無線チャネル容量内に多数の加入者を受容するために音声を圧縮して伝送する。音声を圧縮するためには音声符号化アルゴリズムを使用しなければならないが、一般に移動通信分野では低伝送率でありながら有線網音質を有するボコーディング（Ｖｏｃｏｄｉｎｇ）アルゴリズムを用いる。ボコーディングアルゴリズムは、誤差があるアルゴリズムであるので圧縮と復元とを繰り返せばするほど復元された音声と原音声との間の誤差は大きくなる。すなわち、復元された音声の音質が低下する。

【０００３】図１は、一般的な移動通信システムにおける移動加入者間の通話時、区間別伝送形態を示した図面である。図示されるように、移動加入者間の通話である時、移動局１、１′で音声を圧縮してパケット形態で伝送局２、２′に伝送すると、伝送局システム内のボコーダ（図示せず）で伝送されたパケットをＰＣＭ（Ｐｕｌｓｅ Ｃｏｄｅ Ｍｏｄｕｌａｔｉｏｎ）形態に復元する。この復元されたＰＣＭデータは交換局３を経て通話しようとする相手側移動局１′、１がサービスを受けている伝送局２′、２に送られて、再び伝送局２′、２内にあるボコーダで再圧縮をする。ここで、前記伝送局２、２′は制御局と基地局とを含む。このように圧縮されたパケットは、無線チャネルを通して移動局１′、１に伝送される。

【０００４】次に、パケットを受信した移動局１、１′は、移動局１、１′内のボコーダでパケットを復元することになり、これにより、移動加入者は相手方の音声を聞くことができる。結局、移動加入者間の通話時には、２回のボコーディング過程を経るようになることが分かる。そして、移動加入者間の通話である場合、移動局１、１′で圧縮されて無線チャネルに伝送されてきた音声パケットをシステム内にあるボコーダでパケットバイパス（Ｐａｃｋｅｔ Ｂｙｐａｓｓ）させることにより、ボコーディング過程を減らすようになり、結局、音質低下を補完できる。また、パケットバイパス機能は、データ通信時にも用いられる。ここで、移動局１、１′と伝送局２、２′との間は無線チャネル区間であり、伝送局２、２′と交換局３との間は有線チャネル区間である。

【０００５】以下、図２を参照して従来技術による音声信号のボコーディング装置に対して説明すると次の通りである。図２は、一般的な移動通信システムにおけるボコーダバイパスされたパケット類型を示した図面であり、図２（ａ）はバイパスされた音声パケットのフォーマットを示した図面であり、図２（ｂ）はバイパスされたデータパケットのフォーマットを示した図面であり、

図３は従来技術による移動通信システムにおける動作モード別ボコーディング装置のブロック構成を示した図面である。

【０００６】まず、移動通信システムにおけるボコーディング装置は、ボコーダ２０と、上位プロセッサ１０とで構成される。ここで、上位プロセッサ１０は、伝送局２、２′と交換局３全体でボコーダ２０を除いた残り部分を総括する部分である。そして、前記ボコーダ２０は、第１、２、３、４モードスイッチング部２２、２６、２７、３１と、各モード別にボコーディングを処理する第１ないし第６ボコーディング処理部２３、２４、２５、２８、２９、３０とで構成される。

【０００７】このような構成を有する従来技術による移動通信システムのボコーディング装置は、移動加入者間通話時３種類のモードで動作する。１番目のモードは、通話しようとする移動加入者端末機内のボコーダが相異なる種類のボコーダの場合、例えば、ＥＶＣＲ（Ｅｎｈａｎｃｅｄ Ｖａｒｉａｂｌｅ Ｃｏｄｅ Ｒａｔｅ）とＱＣＥＬＰ（Ｑｕａｌｃｏｍｍ Ｃｏｄｅ Ｅｘｃｉｔｅｄ Ｌｉｎｅａｒ Ｐｒｅｄｉｃｔｉｖｅ）間、８Ｋｂｐｓ ＱＣＥＬＰと１３ＫｂｐｓＱＣＥＬＰ間である時であり、システムのボコーダは、正常なボコーディング（音声符号化と復号化）過程を遂行する。この時、無線チャネル（端末機とシステムボコーダとの間の伝送路）上ではパケット形態で通信され、有線チャネル（交換局を間に置いたシステムボコーダ間伝送路）上の伝送形態はＰＣＭである。

【０００８】２番目のモードは、通話しようとする移動加入者端末機のボコーダが相互に同一な場合であり、例えば、ＥＶＣＲとＥＶＣＲまたはＱＣＥＬＰとＱＣＥＬＰの時であり、システムのボコーダは、音声パケットバイパス（Ｖｏｉｃｅ Ｐａｃｋｅｔ Ｂｙｐａｓｓ）モードで動作する。この時は、無線チャネル上でパケット形態で取り交わし、有線チャネル上における伝送形態は、図２（ａ）に示されたようなバイパスされた音声パケットである。

【０００９】そして、三番目のモードは、移動加入者間データ通信をする場合であり、システムボコーダは、データパケットバイパス（Ｄａｔａ Ｐｃｋｅｔ Ｂｙｐａｓｓ）モードで動作する。この時、無線チャネル区間はパケット形態で取り交わし、有線チャネル区間は図２（ｂ）のようなバイパスされたデータパケット形態で伝送する。

【００１０】このように前記した３種類のモードで動作を遂行する従来ボコーディングシステムは図３に示された通りである。図３に示したように、ボコーダ２０は、上位プロセッサ１０から３種類のモード中、一種類のモードで動作できるモード情報Ｅを受けてモード制御器２１で各モードに合う動作を制御する。すなわち、上位プロセッサ１０から前記１番目のモード情報が入力されると、モード制御器７は、スイッチング部２２、２６を第１ボコーディング処理部２３にスイッチングして移動端末機から無線チャネルＡを通して伝送されてきた音声パケットをＰＣＭにボコーディングしてＰＣＭデータを交換局に有線チャネルＣを通して伝送する。

【００１１】また、モード制御器２１は、スイッチング部２７、３１を第４ボコーディング処理部２８にスイッチングさせて交換局から有線チャネルＤを通して伝送したＰＣＭデータをパケットデータにボコーディングして無線チャネルＢを通して通話しようとする移動端末機に伝送することになる。

【００１２】一方、上位プロセッサ１０から前記二番目のモード情報が入力されると、モード制御器７は、スイッチング部２２、２６を第２ボコーディング処理部２４にスイッチングして移動端末機から無線チャネルＡを通して伝送した音声パケットをバイパスさせて、そのバイパスされた音声パケットデータを有線チャネルＣを通して交換局に伝送する。

【００１３】また、モード制御器２１は、スイッチング部２７、３１を第５ボコーディング処理部２９にスイッチングして交換局から有線チャネルＤを通して伝送された音声パケットデータをバイパスさせてバイパスされた音声パケットデータを無線チャネルＢを通して通話しようとする移動端末機に伝送することになる。

【００１４】また、上位プロセッサ１０から前記三番目のモード情報が入力されると、モード制御器７は、スイッチング部２２、２６を第３ボコーディング処理部２３にスイッチングして移動端末機から無線チャネルＡを通して伝送されたデータパケットをバイパスさせてバイパスされたデータパケットを交換局に有線チャネルＣを通して伝送するようにする。

【００１５】また、モード制御器２１は、スイッチング部２７、３１を第６ボコーディング処理部３０にスイッチングして交換局から有線チャネルＤを通して伝送したデータパケットをバイパスさせてバイパスされたデータパケットを無線チャネルＢを通して通話しようとする移動端末機に伝送する。

【００１６】前記のように、ボコーダ２０は、上位プロセッサ１０とモード情報のみならず無線チャネルＡ、Ｂ上を通信するパケットを取り交わし、モード情報により適切な処理過程を遂行し、有線チャネルＣ、Ｄ区間ではモードにより図２に示された形態のようなバイパスされたパケット及びＰＣＭなどを入出力する。

【００１７】そして、上位プロセッサ１０は、ボコーダ２０を制御する役割だけでなく無線チャネルを通して移動局とシステムボコーダ間のパケット通信をするようにする。

【００１８】

【発明が解決しようとする課題】このような従来技術によるボコーディングシステムにおいて、システムボコー

ダが前記各モードで動作する時、特に有線チャネル上で盗聴が容易にできる問題点がある。すなわち、前記第１番目のモードで動作する場合（ボコーディングモードで動作する場合）、有線チャネル区間で伝送されるＰＣＭは、盗聴装備により容易に盗聴できる。

【００１９】そして、２番目のモード、すなわち、音声パケットバイパスモードで動作する場合は、一般のＰＣＭ盗聴方法では盗聴できないが、図２（ａ）で示したように、純粋音声パケットが予め定義されたフィールドに定まった順序通りに位置しているためにバイパスされた音声パケット全体から音声パケットを探すことができる位置に対する場合の数は非常に制限的であるため、容易に盗聴されることがある。

【００２０】また、前記と類似した３番目のモード、すなわち、データパケットバイパスモードでも、図２（ｂ）に示されたようにバイパスされたデータパケットが有線チャネル上で繰り返して表れることになり、同一のパターンを有するフラグフィールド（Ｆｌａｇ Ｆｉｅｌｄ）を除去してしまえば、容易に純粋データパケットを抽出することができるので、盗聴が容易な短所がある。

【００２１】本発明は前記のような問題点を解決するために提案されたもので、本発明の目的は、伝送側システムボコーダ内に暗号化機能を置いて有線チャネル上に伝送しようとする通信信号を暗号化して伝送し、受信側システムボコーダ内には暗号化されたデータを復号化することができる解読機能を置いて通信信号を解読できるようにして盗聴を防止できるようにした移動通信システムにおける音声及びデータ暗号化復号化装置を提供することにある。また、本発明の他の目的は、前記ボコーディング装置の動作と相応する音声及びデータ暗号化／復号化方法を提供することにある。さらに詳細には、有線チャネル区間で音声盗聴及びデータの流出を防ぐため保安性を高める必要があり、このためにシステムボコーダ内に暗号化器と解読器とをすべて設けて上位プロセッサから提供される同一の暗号化キーを利用して通信信号を暗号化して受信される暗号化された通信信号を解読できるようにした移動通信システムにおける音声及びデータ暗号化／復号化装置及びその方法を提供することにある。

【００２２】

【課題を解決するための手段】前記のような目的を達成するための本発明による移動通信システムにおける音声及びデータ暗号化装置の特徴は、音声及びデータの動作モードを制御する動作モード制御信号、データ暗号化のための暗号化キー供給制御信号及び同期信号発生制御信号を生じる制御部と、前記制御部から発生した動作モード制御信号により無線チャネル区間から伝送されてきた音声／データパケットをボコーディングしたりバイパスさせる動作モード処理部と、前記制御部から発生した暗号化キー供給制御信号によりランダムナンバーを発生させるランダムナンバー発生部と、前記制御部から発生した同期信号発生制御信号により同期信号を生じて有線チャネル区間に伝送する同期信号伝送部と、前記ランダムナンバー発生部から発生したランダムナンバーを利用して前記動作モード処理部でボコーディングまたはバイパスされたＰＣＭまたは音声／データパケットを暗号化した後、前記同期信号の伝送が完了すると、有線チャネル区間に伝送する暗号化部とで構成される。

【００２３】また、本発明による移動通信システムで音声及びデータ復号化装置の特徴は、有線チャネル区間から伝送されてきた暗号化された信号から同期信号を検出する同期信号検出部と、前記同期信号検出部から同期信号が検出されると、前記復号化制御信号及び動作モード制御信号を提供して、復号化キーを供給できるように制御信号を提供する制御部と、前記制御部から提供される復号化キーによりランダムナンバーを生じるランダムナンバー発生部と、前記制御部から提供される復号化制御信号により前記ランダムナンバー発生部から発生したランダムナンバーで有線チャネルから受信された暗号化された信号を復号化する復号化部と、前記制御部から提供される動作モードにより前記復号化部で復号化されたＰＣＭをボコーディングしてパケットに変換したりまたは音声／データパケットをそのままバイパスさせた後、無線チャネル区間に伝送する動作モード処理部とで構成される。

【００２４】また、本発明による移動通信システムにおける音声及びデータ暗号化方法の特徴は、無線チャネル区間から伝送されてきた音声パケットまたはデータパケットを提供される動作モードによりボコーディングまたはバイパスさせた後出力する段階と、暗号化キー情報により任意の一定なランダムナンバーを生じる段階と、同期信号を生成してその生成した同期信号を有線チャネル区間に伝送する段階と、前記同期信号が伝送されると前記発生したランダムナンバーを利用して前記モード処理された信号（ＰＣＭまたはバイパスされた音声パケットまたはバイパスされたデータパケット）を暗号化した後、暗号化された信号を有線チャネル区間に伝送する段階とで構成される。

【００２５】また、本発明による移動通信システムで音声及びデータ復号化方法の特徴は、有線チャネル区間から暗号化された信号を受信する段階と、暗号化された信号が受信されると、その暗号化された信号から同期信号を検出する段階と、前記同期信号が検出されると、復号化キーにより任意の一定なランダムナンバーを生じる段階と、前記発生したランダムナンバーにより前記暗号化された信号を復号化する段階と、前記復号化されたＰＣＭまたはパケットを動作モードによりボコーディングまたはバイパスさせてパケットに変換した後、無線チャネル区間に伝送する段階とで構成される。

【００２６】

【発明の実施の形態】以下、本発明による移動通信システムにおける音声及びデータ暗号化／復号化装置及びその方法に対して添付した図面を参照して詳細に説明すると次の通りである。まず、本発明は、前記従来技術で説明したように移動加入者間通話時ボコーダの動作モードにより有線チャネル区間で伝送される通信信号の類型はすべて3種類である。すなわち、音声通話時ボコーダがボコーディングモードで動作する場合ＰＣＭであり、音声パケットバイパスモードで動作する場合にはバイパスされた音声パケットである。そして、データ通信時に、ボコーダはデータパケットバイパスモードで動作し、有線チャネル区間ではバイパスされたデータパケット形態である。本発明は前記のようなあらゆる類型に対して暗号化及び復号化が可能にする。

【００２７】図４は、本発明による移動通信システムにおける音声／データを暗号化して解読するボコーディングシステムのブロック構成を示した図面である。図示されるように、動作モード情報及び暗号化キー情報を提供する上位プロセッサ３０と、上位プロセッサ３０から提供されるモード情報により入力される端末機で無線チャネルＡを通して伝送した音声またはデータパケットをボコーディングまたはバイパスモードで動作処理して、デスクランブリングされた信号をパケットにボコーディングしたりまたはバイパスモードで動作処理してパケットを無線チャネルＢを通して移動端末機に伝送する動作モード処理部４１と、上位プロセッサ３０で提供する暗号化キー情報を貯蔵及び貯蔵された暗号化キー情報を出力させるための制御信号、同期信号伝送制御信号及びスイッチング制御信号を各々発生して提供する制御部４２と、制御部４２から提供される貯蔵制御信号により上位プロセッサ３０から提供される暗号化キー情報を貯蔵して、出力制御信号により貯蔵された暗号化キー情報を出力する暗号化キーシード（Ｓｅｅｄ）部４５で構成される。

【００２８】また、制御部４２から提供される制御信号により一般モードまたは暗号化モードにスイッチング転換する第１スイッチング部４３と、暗号化キーシード部４５から提供される暗号化キー情報によりランダムナンバー（Ｒａｎｄｏｍ Ｎｕｍｂｅｒ）を発生させるランダムナンバー発生部４６と、ランダムナンバー発生部４６から発生したランダムナンバーにより動作モード処理部４１を通してモード処理（ボコーディングまたはバイパス）されたパケットまたはＰＣＭ信号を暗号化（Ｓｃｒａｍｂｌｉｎｇ）するスクランブリング部４７と、制御部４２から提供される同期信号伝送制御信号により同期信号を発生して、発生された同期信号を伝送する同期信号伝送部４４と、前記同期信号伝送部４４から伝送された同期信号を先に伝送して、スクランブリング部４７出力端にスイッチングしてスクランブリング部４７でスクランブルされた信号をスイッチングして暗号化されたデータを有線チャネルＣを通して交換局に伝送する第２スイッチング部４８とで構成される。

【００２９】また、有線チャネルＤを通して受信される暗号化された信号から同期信号を検出する同期信号検出部４９と、同期信号検出部４９から同期信号が検出されると、制御部４２の制御信号により一般モードから解読モードにスイッチング転換する第３スイッチング部５０と、第３スイッチング部５０のスイッチングにより受信された暗号化された信号を解読（Ｄｅｓｃｒａｍｂｌｉｎｇ）した後、前記動作モード処理部４１に出力するデスクランブリング部５１とで構成される。

【００３０】このような構成を有する本発明による移動通信システムにおける音声／データ暗号化／復号化装置の詳細動作を説明すると次の通りである。まず、ボコーダ４０は、上位プロセッサ３０から動作モードＥ及び暗号キー情報Ｆを受ける。そうすれば、ボコーダ４０の動作モード処理部４１及び制御部４２で制御信号を生成する。

【００３１】すなわち、制御部４２は、暗号キーを暗号化シード部４５に貯蔵させた後、貯蔵された暗号化キーをリードしてランダムナンバー発生部４６に出力させる。この時、制御部４２は第１スイッチング部４３をａ端からｇ端にスイッチング転換させるようになる。

【００３２】そして、ランダムナンバー発生部４６は、暗号キーシード部４５から提供される暗号化キーにより任意のランダムナンバーを生じてスクランブリング部４７に提供する。

【００３３】したがって、スクランブリング部４７は、第１スイッチング部４３のスイッチング転換により動作モード処理部４１から出力されるバイパスされたパケットまたはボコーデングされたＰＣＭ信号をランダムナンバー発生部４６から提供されるランダムナンバーによりスクランブル、すなわち、暗号化させた後、第２スイッチング部４８に出力する。

【００３４】この時、制御部４２は、同期信号伝送部４４に制御信号を提供すると同時に第２スイッチング部４８にスイッチング制御信号を提供して同期信号伝送部４４で発生した同期信号を有線チャネル区間に先に伝送する。同期信号が伝送されると、制御部４２は、第２スイッチング部４８をスクランブリング部４７にスイッチング転換させて、スクランブリング部４７で暗号化された信号を有線チャネル区間に伝送するようになる。

【００３５】ここで、同期信号は、最初のフレームに対する暗号化された信号を有線チャネル区間に伝送する前に１回のみ伝送するようになり、その以後のあらゆるフレームに対しては同期信号を伝送しなくなる。

【００３６】一方、有線チャネル区間で前記のように暗号化されたデータが受信されると、ボコーダ４０の同期信号検出部４９では受信された暗号化された信号から同期信号を検出して同期信号検出結果を制御部４２に提供

する。この時、制御部４２は、同期信号検出部４９から同期信号が検出されると、第３スイッチング部５０をｄ端からｉ端にスイッチング転換させる。

【００３７】したがって、受信された暗号化された信号、すなわち、スクランブリングされた信号はスクランブリングの逆過程、すなわち、ランダムナンバー発生部４６から出力されるランダムナンバーにより解読される。このように解読されたパケットまたはＰＣＭ信号は動作モード処理部４１に提供される。

【００３８】動作モード処理部４１は、上位プロセッサ３０から提供される動作モードによりボコーディングまたはバイパス動作を遂行してバイパスされたパケットまたはボコーデングされたＰＣＭを無線チャネル区間に伝送するようになる。

【００３９】前記暗号化及び復号化機能に対してさらに詳細に説明すると次の通りである。ボコーダ４０は、上位プロセッサ３０から動作モード及び暗号化キー情報を受ける。ボコーダ４０は、この情報で動作モード処理部４１及び制御部４２で制御信号を作る。すなわち、制御部４２は、暗号キーを暗号化シード部４５に貯蔵させた後、貯蔵された暗号化キーをランダムナンバー発生部４６に出力させる。

【００４０】これにより、ランダムナンバー発生部４６は、暗号化シード部４５から提供される暗号化キーによりランダムナンバーを発生させる。この時、ランダムナンバーは、ボコーダ４０の入出力通信信号を暗号化したり解読する情報として用いられる。この情報は、ボコーダ４０の入出力通信信号の位置情報に該当し、暗号化を遂行するスクランブリング部４７と解読を遂行するデスクランブリング部５１とに各々入力される。

【００４１】スクランブリング部４７は、ランダムナンバー発生部４６から発生した位置情報を利用して動作モード処理部４１から出力された通信信号ｇの各位置をビットまたはバイト単位で再配列する。この時、暗号化の程度は暗号化しようとする通信信号をバイト単位で再配列することよりはビット単位で再配列することがさらに性能が優れる。このように、再配列された信号ｈをスクランブリング部４７は同期信号伝送部４４から発生した同期信号と合成してボコーダ４０出力端Ｃに出力することにより、暗号化された信号が有線チャネル上に伝送される。

【００４２】そして、デスクランブリング部５１は、有線チャネル区間から伝送されてきた暗号化された信号Ｄをランダムナンバー発生部４６から発生した位置情報を利用して下記表１のスクランブリング過程の逆過程で信号を逆配列することにより、元来の信号ｊを解読する。この過程に対する例を下の表１を参考にして説明すると次の通りである。

【００４３】

【表１】

原位置	0	1	2	3	4	5	6	7	8	9
通信信号	Ｘ０	Ｘ１	Ｘ２	Ｘ３	Ｘ４	Ｘ５	Ｘ６	Ｘ７	Ｘ８	Ｘ９
ランダムナンバー	1	3	5	7	2	9	8	4	6	0
再配列信号	Ｘ１	Ｘ３	Ｘ５	Ｘ７	Ｘ２	Ｘ９	Ｘ８	Ｘ４	Ｘ６	Ｘ０

【００４４】説明の便宜上、１０バイト単位で通信信号ｇを再配列（暗号化）しようとするならば、０－９間の１０個のランダムナンバーｋを発生させる。前記の表１のように任意のランダムナンバーが発生したならば、第１番目のランダムナンバーが１であるために１の位置にある通信信号Ｘ１を第１番目の位置（位置０）にもってくる。そして、二番目のランダムナンバーが３であるために３の位置にあった通信信号Ｘ３を二番目位置（位置１）にもってくる。こういう方法で最後の九番目ランダムナンバーは０であるために０の位置にある通信信号Ｘ０を位置（位置９）に移動させる。結局、このようにすれば、一番下の再配列された信号が得られるようになり、これが暗号化された信号になる。解読過程（デスクランブリング）は、前記暗号化過程を逆に遂行すれば、容易に元来の通信信号を逆配列できることが分かる。

【００４５】ところで、システムの伝送側と受信側との各ボコーダが暗号化された信号を正確に解読するためには暗号化及び解読を始める時点が一致しなければならない。すなわち、システムボコーダ間有線チャネル区間で通信信号の伝送遅延に対して考慮しなければならない。これを解決する方法としていろんな方法が有り得るが、システムの設計及び形状により変わる場合がある。ここではいかなるシステムの構造でも動作できる方法として、スクランブリング部４７及びデスクランブリング部５１が動作する時点に対する同期情報をスクランブリング部４７で暗号化された信号を伝送する前に同期信号伝送部４４から第２スイッチング部４８を通して有線チャネルを通して伝送する。

【００４６】また、これと並行して有線チャネルＤから受信される同期情報を先に検出した後、同期情報が検出されると受信された暗号化された信号をデスクランブリング部５１で前記したような解読方法により解読する。

【００４７】したがって、有線チャネル上で伝送側ボコーダと受信側ボコーダとの間の通信信号伝送遅延で生じ

るスクランブリング部４７とデスクランブリング部５１との駆動時点に対する不一致を解決することができ、同一暗号キーを利用した通信信号の暗号化及び暗号化された信号の解読機能を正確に遂行できるようになる。この時、前記同期情報は予め約束された一定パターンで構成される。

【００４８】以下、添付された図５及び図６を参照して本発明による移動通信システムの音声／データ暗号化方法及び復号化方法を各々区分して段階的に説明すると次の通りである。まず、図５を参照して移動通信システムで音声／データ暗号化方法に対して説明すると次の通りである。まず、無線チャネル区間から伝送されてきた音声パケットまたはデータパケットを上位プロセッサ３０から提供される動作モードにより該モードを遂行する（Ｓ１０１）。すなわち、受信される音声パケットを提供される動作モードによりボコーディングしてＰＣＭに変換したり、音声パケットをバイパスさせたり、またはデータパケットをバイスパスさせる。

【００４９】次に、上位プロセッサ３０から提供される暗号化キー情報により任意の一定なランダムナンバーを生じる（Ｓ１０２）。同時に提供される制御信号により同期信号を生じて、その発生した同期信号を有線チャネル区間に伝送した後（Ｓ１０３）、同期信号の伝送が完了すると前記発生したランダムナンバーを利用して前記モード処理された信号（ＰＣＭまたはバイパスされた音声パケットまたはバイパスされたデータパケット）を暗号化する（Ｓ１０４）。このように暗号化された信号を有線チャネル区間に伝送する（Ｓ１０５）。

【００５０】そして、図６を参照して有線チャネル区間から伝送されてきた暗号化された信号を解読する方法に対して段階的に説明すると次の通りである。まず、有線チャネル区間から暗号化された信号が受信されているかを判断する（Ｓ２０１）。その判断結果、暗号化された信号が受信されると受信された暗号化された信号から同期信号を検出する（Ｓ２０２）。

【００５１】その後、段階Ｓ２０３で同期信号が検出されるのかを判断して、その判断結果、同期信号が検出されると、提供される解読キーにより任意の一定なランダムナンバーを生じる（Ｓ２０４）。続いて、前記発生したランダムナンバーにより前記受信された暗号化された信号を解読（Ｄｅｓｃｒａｍｂｌｉｎｇ）した後（Ｓ２０５）、解読された信号、すなわち、ＰＣＭまたはパケットを提供される動作モードにより該モードを遂行した後、モード処理されたパケットを無線チャネル区間に伝送する（Ｓ２０６）。ここで、該モードは、解読されたＰＣＭをパケットに変換したり、または解読されたパケットをバイパスさせる動作を示す。

【００５２】

【発明の効果】以上詳述したように、本発明による移動通信システムで音声／データの暗号化／復号化装置及びその方法は、無線チャネル区間から伝送されてきた信号をボコーディングまたはバイパスさせた後、ボコーディングまたはバイパスされた信号をランダムナンバーを利用してスクランブリングして有線チャネル区間に伝送して、有線チャネル区間から受信されるスクランブリングされた信号をデスクランブリングした後、ボコーディングまたはバイパスさせて無線チャネル区間に伝送することにより、システムボコーダ間有線チャネル区間における保安性を画期的に維持させ盗聴を未然に防止することができる利点がある。また、今後、移動端末機とボコーダとの間の無線チャネル区間まで拡張して全チャネル上で保安性を保障できる効果を有する。

【図面の簡単な説明】

【図１】　一般的な移動通信システムで移動加入者間の通話時、区間別伝送形態を示した図面である。

【図２】　一般的な移動通信システムでボコーダバイパスされたパケット類型を示した図面であり、（ａ）はバイパスされた音声パケットのフォーマットを示した図面、（ｂ）はバイパスされたデータパケットのフォーマットを示した図面である。

【図３】　従来技術による移動通信システムにおける動作モード別ボコーディング装置のブロック構成を示した図面である。

【図４】　本発明による移動通信システムにおける音声及びデータ暗号化／復号化装置のブロック構成を示した図面である。

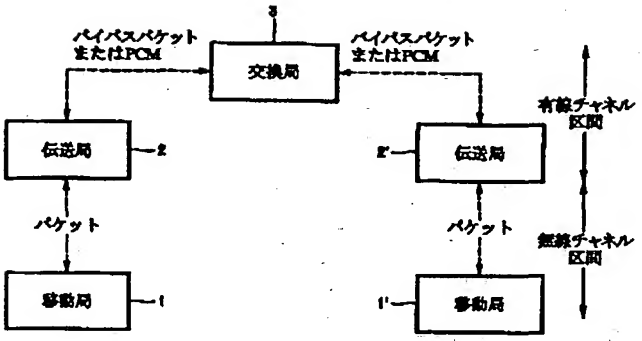
【図５】　本発明による移動通信システムで音声及びデータ暗号化／復号化方法を示した流れ図である。

【図６】　本発明による移動通信システムで音声及びデータ暗号化／復号化方法を示した流れ図である。

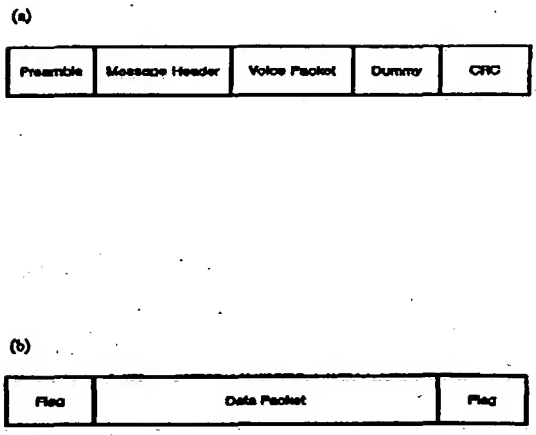
【符号の説明】

３０　上位プロセッサ、４０　ボコーダ、４１　動作モード処理部、４２　制御部、４３、４８、５０　スイッチング部、４４　同期信号伝送部、４５　暗号化シード部、４６　ランダムナンバー発生部、４７　スクランブリング部、４９同期信号検出部、５１　デスクランブリング部。

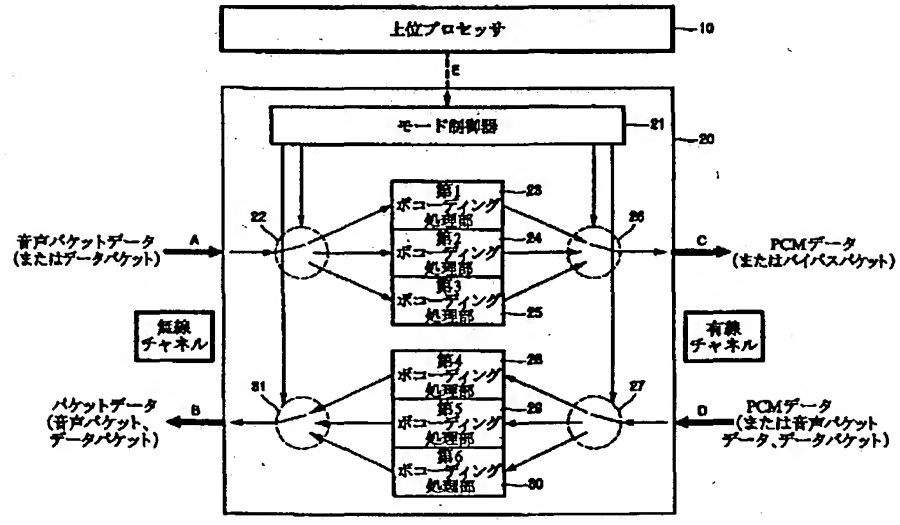
【図１】


3
バイパスパケット
またはPCM
交換局
バイパスパケット
またはPCM
有線チャネル
区間
伝送局
2
2'
伝送局
パケット
パケット
無線チャネル
区間
移動局
1
1'
移動局

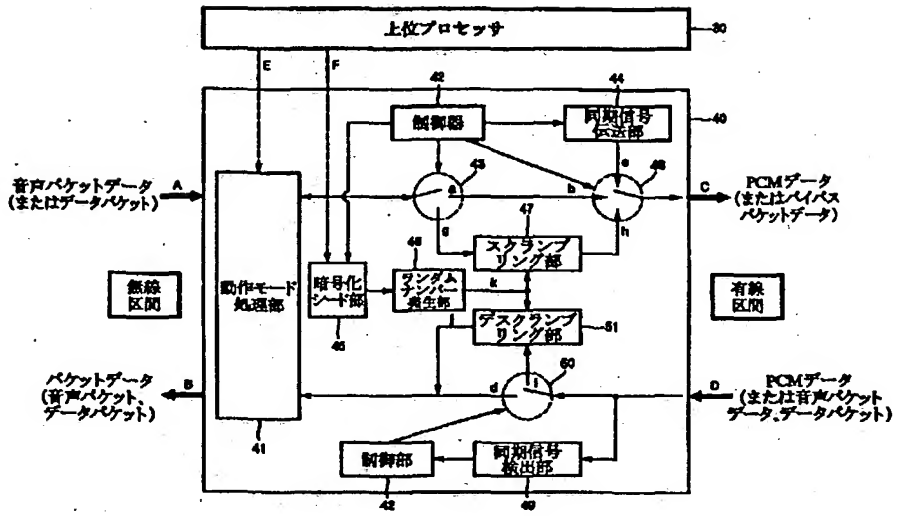
【図２】


(a)
Preamble
Message Header
Voice Packet
Dummy
CRC
(b)
Flag
Data Packet
Flag

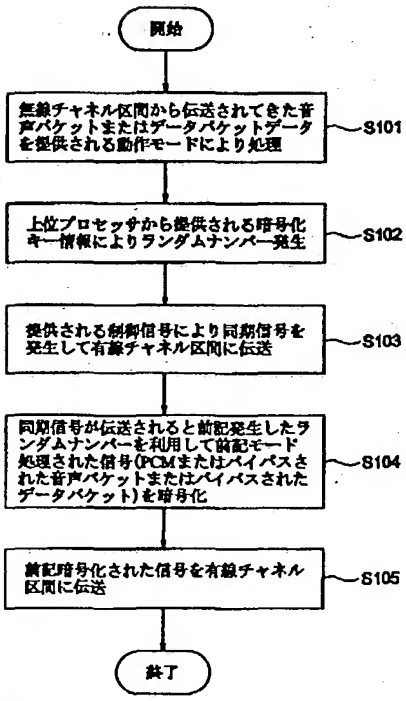
【図３】


上位プロセッサ
10
E
モード制御器
21
20
第1
ボコーディング
処理部
23
第2
ボコーディング
処理部
24
第3
ボコーディング
処理部
25
22
26
音声パケットデータ
(またはデータパケット)
A
C
PCMデータ
(またはバイパスパケット)
無線
チャネル
有線
チャネル
第4
ボコーディング
処理部
28
第5
ボコーディング
処理部
29
第6
ボコーディング
処理部
30
31
27
パケットデータ
(音声パケット、
データパケット)
B
D
PCMデータ
(または音声パケット
データ、データパケット)

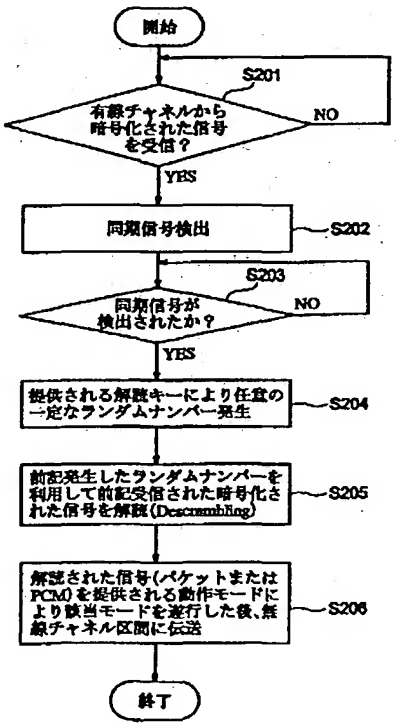
【図４】


上位プロセッサ
30
E
F
42
44
制御器
同期信号伝送部
40
43
46
音声パケットデータ（またはデータパケット）
A
PCMデータ（またはバイパスパケットデータ）
C
47
スクランブリング部
48
暗号化シード部
ランダムナンバー発生部
無線区間
動作モード処理部
有線区間
51
デスクランブリング部
50
パケットデータ（音声パケット、データパケット）
B
PCMデータ（または音声パケットデータ、データパケット）
D
41
制御部
同期信号検出部
42
49

【図５】


開始
無線チャネル区間から伝送されてきた音声パケットまたはデータパケットデータを提供される動作モードにより処理
S101
上位プロセッサから提供される暗号化キー情報によりランダムナンバー発生
S102
提供される制御信号により同期信号を発生して有線チャネル区間に伝送
S103
同期信号が伝送されると前記発生したランダムナンバーを利用して前記モード処理された信号(PCMまたはバイパスされた音声パケットまたはバイパスされたデータパケット)を暗号化
S104
前記暗号化された信号を有線チャネル区間に伝送
S105
終了

【図６】


開始
S201
有線チャネルから暗号化された信号を受信？
NO
YES
同期信号検出
S202
S203
同期信号が検出されたか？
NO
YES
提供される解読キーにより任意の一定なランダムナンバー発生
S204
前記発生したランダムナンバーを利用して前記受信された暗号化された信号を解読(Descrambling)
S205
解読された信号(パケットまたはPCM)を提供される動作モードにより該当モードを遂行した後、無線チャネル区間に伝送
S206
終了